P27325.A13

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of	Docket No.: P27325
J. L. CALVIGNAC et al.	Confirmation No.: 6208
Serial No.: 09/771,472	Group Art Unit: No. 2134
Filed: January 26, 2001	Examiner: E. C. Tran

For: **SINGLE-CYCLE HARDWARE IMPLEMENTATION OF CRYPTO FUNCTION FOR HIGH THROUGHPUT CRYPTO-PROESSING**

REPLY BRIEF UNDER 37 C.F.R. 41.41(a)(1)

Commissioner for Patents
U.S. Patent and Trademark Office
Customer Service Window, Mail Stop **Appeal Brief - Patents**
Randolph Building
401 Dulany Street
Alexandria, VA 22314
Sir:

This Reply Brief is in response to the Examiner's Answer dated March 28, 2007, the period for reply extending until May 29, 2007.

The Examiner maintains the grounds of rejection advanced in the final rejection of claims 1-20 and provides arguments in support thereof.

Appellant notes this Reply Brief is being filed under 37 C.F.R. 41.41(a)(1) and is directed to the arguments presented in the Examiner's Answer, and therefore must be entered unless the final rejection is withdrawn in response to the instant Reply Brief. With regard to this Reply Brief, Appellant notes it is addressing points made in the Examiner's Answer and not repeating the arguments set forth in the Appeal Brief.

POINTS OF ARGUMENT

First Issue

On the pages 4 and 5 of the Examiner's Answer, the Examiner explains how claim 1 can be broadly and reasonably interpreted so as to be rendered anticipated by GREENE. Appellant submits that the Examiner's interpretations of certain features of claim 1 are neither reasonable nor supported by the disclosure of GREENE.

> Claim 1 recites a hardware implementation of a crypto-function comprising:
> a first register storing data to be encrypted or decrypted;
> a second register for receiving data which has been encrypted or decrypted; and
> combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle. Emphasis Added.

The specification defines combinational logic as "logic functions whose outputs depend solely on their inputs. These are logic circuits without memory." This language is further clarified by the following language in the specification. "In contrast to prior hardware implementations of crypto-functions, there are no registers to store intermediate results, or iterations, of the enciphering or deciphering computations." (see page 2, lines 14-18 of the specification).

Appellant submits that the Examiner muddies the waters by failing to specifically and consistently identify the features of GREENE which the Examiner believes equates to each recited feature, and by taking at least three different positions on claim interpretation. Appellant will illustrate this with reference to Fig. 1 of GREENE.

According to one position of the Examiner, the working store 104 of GREENE is the recited first register, the output buffer 108 is the recited second register, and the

encryption circuit 102 is the recited combinational logic. This interpretation, while improper, is the more reasonable of the three positions. The reason it is improper, however, is that GREENE does not explain the detailed function of the encryption circuit 102 (i.e., the so-called combinational logic) in any language which could arguable be characterized as the recited combinational logic. On the other hand, claim 1 specifically recites that the combinational logic performs computation iterations of the crypto-function on data stored in the first register and outputs data to said second register in a single hardware cycle. Since the Examiner has not identified any language in GREENE which specifically explains that the encryption circuit 102 (i.e., the so-called combinational logic) performs computation iterations of the crypto-function on data stored in the first register and outputs data to said second register in a single hardware cycle, this interpretation is unsupported by the disclosure of GREENE, and therefore improper.

According to another position of the Examiner, the entire circuit shown in Fig. 1 of GREENE somehow teaches the recited first register, the recited second register, and, more specifically, the recited combinational logic. This interpretation is convenient for the Examiner apparently because the Examiner need not identify which specific features of Fig. 1 of GREENE equate to each recited feature. However, the reason that this interpretation is improper is that the circuit shown in Fig. 1 utilizes devices such as the working store 104 and the output buffer 108 which are disclosed as including storage circuits (see col. 5, lines 13-15 and 24-28). As Appellant has defined the combinational

logic as "logic functions whose outputs depend solely on their inputs. These are logic circuits without memory. In contrast to prior hardware implementations of crypto-functions, there are no registers to store intermediate results, or iterations, of the enciphering or deciphering computations." Emphasis Added. (see page 2, lines 14-18 of the specification), such an interpretation cannot be reconciled. Furthermore, even if the Examiner were correct that the whole circuit of Fig. 1 of GREENE equates to the recited combinational logic, the Examiner has not explained how this circuit performs computation iterations of the crypto-function on data stored in the first register and outputs data to said second register in a single hardware cycle.

According to still another position of the Examiner, the devices 106 and 102 of the circuit shown in Fig. 1 of GREENE constitute the recited combinational logic. This interpretation is also convenient for the Examiner apparently because the Examiner need not identify which specific functions of devices 106 and 102 equates to the recited combinational logic. However, the reason that this interpretation is it improper is that GREENE merely explains that device 106 is a scheduler and that device 102 is an encryption circuit. However, conspicuously absent from any of the discussion in GREENE is any language even remotely disclosing that the devices 106 and 102 (i.e., the recited combinational logic) perform computation iterations of the crypto-function on data stored in the first register and outputs data to said second register in a single hardware cycle. The Examiner's mere conclusions to the contrary are simply unavailing.

Second Issue

On the page 5 of the Examiner's Answer, the Examiner asserts that it is reasonable to broadly interpret the language "combinational logic performing computation iterations of the crypto-function on data" (claim 1) as equating to the language "the data blocks that can be pipelined across one or more encryption circuits" allegedly disclosed in GREENE. Appellant disagrees. As explained above, Appellant has defined combinational logic as "logic functions whose outputs depend solely on their inputs. These are logic circuits without memory. In contrast to prior hardware implementations of crypto-functions, there are no registers to store intermediate results, or iterations, of the enciphering or deciphering computations." Emphasis Added. (see page 2, lines 14-18 of the specification). The language "the data blocks that can be pipelined across one or more encryption circuits" is silent with regard to logic functions whose outputs depend solely on their inputs and/or using logic circuits without memory, and/or hardware implementations of crypto-functions without registers to store intermediate results, or iterations, of the enciphering or deciphering computations. As such, the language cited by the Examiner simply cannot reasonably be interpreted as the recited combinational logic. Nor does the noted language disclose anything approaching the language explaining that the combinational logic performs computation iterations of the crypto-function on data stored in the first register and outputs data to said second register in a single hardware cycle. Again, the Examiner's mere conclusions to the contrary are unavailing.

Third Issue

On the page 5 of the Examiner's Answer, the Examiner asserts that it is reasonable to broadly interpret the language "in a single hardware cycle" (claim 1) as equating to "where a cycle can be as small as one clocked cipher stage within an encryption circuit" recited in GREENE. Appellant disagrees. As a preliminary matter, Appellant notes that the Examiner has failed to consider all of the language of this limitation. Appellant has not merely recited "in a single hardware cycle". Instead, claim 1 recites that the combinational logic performs computation iterations of the crypto-function on data stored in the first register and outputs data to said second register in a single hardware cycle. As explained above, GREENE lacks the recited combination logic as defined by Appellant. Furthermore, the language "where a cycle can be as small as one clocked cipher stage within an encryption circuit" says noting about combinational logic, much less, anything which is defined as "logic functions whose outputs depend solely on their inputs. These are logic circuits without memory. In contrast to prior hardware implementations of crypto-functions, there are no registers to store intermediate results, or iterations, of the enciphering or deciphering computations." (see page 2, lines 14-18 of the specification).

Fourth Issue

On the pages 14 and 15 of the Examiner's Answer, the Examiner asserts that the features of claim 5 can be broadly interpreted as "the scheduler programmed to provide feedback encryption operations with a $E^{KB}[b3]$." Appellant disagrees and submits that

this assertion is not supported by any disclosure in GREENE.

Appellant submits that such arguments are improper for at least two reasons. First, the Examiner has not explained why or how certain language of GREENE can be broadly interpreted to disclose the claim features. Second, the Examiner's assertions do not appear to be well supported. Claim 5, for example, specifically recites that the combinational logic performs an invertible key-dependent round function iterated a predetermined number of times. The Examiner merely responds that this language equates to "the scheduler programmed to provide feedback encryption operations with a $E^{KB}[b3]$", but does not indicate how the cited language equates with the claim features. Appellant submits that the cited language provides insufficient disclosure of the claim features.

As is clear from Fig. 1 of GREENE, the scheduler 106 is not part of the encryption circuit 102 and is disclosed in GREENE as determining the order in which data stored in buffer 104 will be processed (see col. 5, lines 32-33). Furthermore, the Examiner has not explained how either the scheduler 106 or the circuit 102 (or their combination) can perform an invertible key-dependent round function iterated a predetermined number of times. At the very least, the Examiner should explain how the noted language of GREENE can be interpreted to disclose a combinational logic performs an invertible key-dependent round function iterated a predetermined number of times. This has clearly not been done. Instead, the Examiner provides sweeping conclusions which are at best unsupported and at worst not understood.

Fifth Issue

Throughout Section 10 (pages 12-17) of the Examiner's Answer, the Examiner attempts to characterize the claims language without addressing each and every limitation and provides mere assertions of anticipation. This is improper.

Appellant directs the Board's attention to MPEP 2131 which specifically states:

> **TO ANTICIPATE A CLAIM, THE REFERENCE MUST TEACH EVERY ELEMENT OF THE CLAIM**
>
> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "When a claim covers several structures or compositions, either generically or as alternatives, the claim is deemed anticipated if any of the structures or compositions within the scope of the claim is known in the prior art." *Brown v. 3M*, 265 F.3d 1349, 1351, 60 USPQ2d 1375, 1376 (Fed. Cir. 2001) (claim to a system for setting a computer clock to an offset time to address the Year 2000 (Y2K) problem, applicable to records with year date data in "at least one of two-digit, three-digit, or four-digit" representations, was held anticipated by a system that offsets year dates in only two-digit formats). See also MPEP § 2131.02. "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim, but this is not an *ipsissimis verbis* test, i.e., identity of terminology is not required. *In re Bond*, 910 F.2d 831, 15 USPQ2d 1566 (Fed. Cir. 1990). Note that, in some circumstances, it is permissible to use multiple references in a 35 U.S.C. 102 rejection. See MPEP § 2131.01.

Rather than complying with the above-noted requirements, the Examiner has instead chosen to ignore claim features and/or mischaracterize the claim features. The Examiner however must, consistent with MPEP 2131, identify <u>each and every element as set forth in the claim is found, either expressly or inherently described</u>. This has not been done in this case.

Furthermore, to the extent that the Examiner is basing the instant rejection on an argument of inherency consistent with MPEP 2112, Appellant notes that MPEP 2112 specifically states, in part:

> "In relying upon the theory of inherency, the examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art." *Ex parte Levy,* 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis in original) (Applicant's invention was directed to a biaxially oriented, flexible dilation catheter balloon (a tube which expands upon inflation) used, for example, in clearing the blood vessels of heart patients). The examiner applied a U.S. patent to Schjeldahl which disclosed injection molding a tubular preform and then injecting air into the preform to expand it against a mold (blow molding). The reference did not directly state that the end product balloon was biaxially oriented. It did disclose that the balloon was "formed from a thin flexible inelastic, high tensile strength, biaxially oriented synthetic plastic material." *Id.* at 1462 (emphasis in original). The examiner argued that Schjeldahl's balloon was inherently biaxially oriented. The Board reversed on the basis that the examiner did not provide objective evidence or cogent technical reasoning to support the conclusion of inherency.).

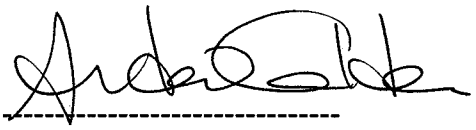
The Examiner has neither stated that the rejection is based on inherency, nor provided any basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art.

CONCLUSION

Accordingly, in view of the above-noted arguments (as well as those already of record), the Board is respectfully requested to reverse the Examiner's decision to finally reject claims 1-20 under 35 U.S.C. §102. Furthermore, the application be remanded to

the Examiner for withdrawal of the rejection over the applied documents and an early allowance of all claims on appeal. The Commissioner is hereby authorized to charge any fees necessary for consideration of this paper to deposit account No. 50-0563.

Respectfully submitted,
J. L. CALVIGNAC et al.



Andrew M. Calderon
Reg. No. 38,093

April 24, 2007
GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
703-716-1191